Please Click here to view the drawing

Korean FullDoc.

(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020010077212 A
(43)Date of publication of application: 17.08.2001

(21)Application number: 1020000004861
(22)Date of filing: 01.02.2000

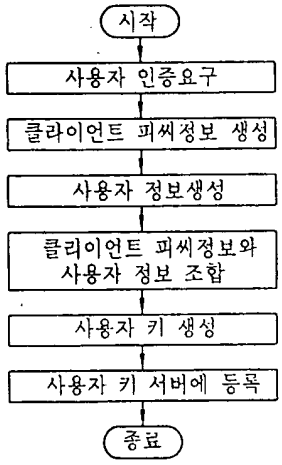
(51)Int. Cl H04L 9 /32

(71)Applicant: LG ELECTRONICS INC.
(72)Inventor: JUNG, CHEOL JONG
PARK, JAE BEOM

(54) METHOD OF GENERATING USER PASSWORD KEY FOR PROTECTING DIGITAL CONTENTS

(57) Abstract:

PURPOSE: A method of generating a user password key for protecting digital contents is provided which authenticates only a specific user using user information and client PC information. CONSTITUTION: On generation of user authentication request, client PC information and user information are created. The client PC information and the user information are combined with each other to generate a corresponding user password key and the user password key is stored in the client PC. The user password key is registered to a server a user wants. The client PC information corresponds to the serial number of the hard disk of the PC. The client PC information is a CPU serial number. The user information is configured of a user ID and user password.



Legal Status
Date of request for an examination (20000201)
Notification date of refusal decision (00000000)
Final disposal of an application (registration)
Date of final disposal of an application (20020718)
Patent registration number (1002486120000)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04L 9/32

(11) 공개번호 특2001-0077212
(43) 공개일자 2001년08월17일

(21) 출원번호 10-2000-0004861
(22) 출원일자 2000년02월01일

(71) 출원인 엘지전자주식회사
구자홍
서울시영등포구여의도동20번지

(72) 발명자 정철종
경기도고양시덕양구화정동928-7201호
박재범
서울특별시서초구양재동74번지현대빌라C동8호

(74) 대리인 박장원

심사청구 : 있음

(54) 디지탈 콘텐츠 보호용 사용자 암호키 생성방법

요약

본 발명은 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법에 관한 것으로, 종래에는 클라이언트 피씨 사용자의 정보만으로 키를 생성할 경우에 그 사용자의 정보가 유출되면 누구나 같은 키를 사용하게 되어 보안이 쉽게 해체되고, 클라이언트 피씨 자체의 정보만으로 키를 생성하는 경우에는 이 클라이언트 피씨를 사용하는 사용자는 누구나 정당한 사용자로 간주되어 보안 유지가 어려운 문제점이 있다. 따라서, 본 발명은 사용자 인증요구가 발생하면 클라이언트 피씨 정보와 사용자 정보를 생성하는 제1 단계와; 상기 클라이언트 피씨 정보와 사용자 정보를 조합하여 그에 따른 사용자 암호키를 생성하여 클라이언트 피씨에 내장하는 제2 단계와; 상기 제2 단계의 사용자 암호키를 사용자가 원하는 서버에 등록하는 제3 단계로 수행함으로써 특정 컴퓨터의 사용자에 의해 생성된 키가 다른 컴퓨터에 복사하더라도 피씨 정보가 틀리므로 처음 키를 생성한 컴퓨터 이외에서는 사용할 수 없고 또한 사용자의 정보가 유출되더라도 최초키를 생성한 컴퓨터가 아니면 동일한 키를 생성할 수 없으므로 확실하게 보안을 유지할수 있고, 그리고 특정 사용자 암호키로 암호화에서 데이터를 전송하면 이 특정 사용자외에는 어느 누구도 데이터를 해독할 수 없으므로 무단 배포를 방지할 수 있는 효과가 있다.

대표도
도 1

명세서

도면의 간단한 설명

도1의 본 발명 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법의 일실시예에 대한 동작흐름도.

도2는 도1에 있어서의 개략적인 모습을 보인도.

도3은 도1에서 생성된 사용자키를 이용한 피씨와 서버사이의 데이터 전송을 보인 개략도.

도4는 본 발명 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법의 다른 실시예에 대한 동작흐름도.

도5는 도4에 있어서의 개략적인 모습을 보인도.

도6은 도4에서 생성된 사용자키를 이용한 피씨와 서버사이의 데이터 전송을 보인 개략도.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 디지탈 콘텐츠 보호용 사용자 암호키 생성방법에 관한 것으로, 특히 클라이언트 피씨 사용자에 대하여 유일한 사용자 암호키를 생성하는 방법에 관한 것이다.

일반적으로, 사용자 암호키를 생성하기 위해서는 클라이언트 피씨 사용자의 정보만으로 사용자 암호키를 생성하거나 클라이언트 피씨 고유의 정보만으로 사용자 암호키를 생성하는데, 이때 상기 클라이언트 피씨 사용자의 정보만으로 사용자 암호키를 생성하는 경우에 사용자 암호키에 대한 보안 책임은 사용자 자신에게 달려있다.

따라서, 사용자가 고의나 불의에 의해 키생성 정보를 유출시키는 경우, 누구나 동일한 키를 생성할 수 있게 되어 정보에 대한 보안이 쉽게 해체된다.

그리고, 상기 클라이언트 피씨의 고유한 정보만을 가지고 사용자 암호키를 생성하는 경우에는 그 클라이언트 피씨를 사용하는 사용자는 누구나 정당한 사용자로 간주되어 특정 사용자에 대한 인증이 불가능하게 된다.

발명이 이루고자 하는 기술적 과제

즉, 상기와 같은 종래 기술에 있어서, 클라이언트 피씨 사용자의 정보만으로 키를 생성할 경우에 그 사용자의 정보가 유출되면 누구나 같은 키를 사용하게 되어 보안이 쉽게 해체되고, 클라이언트 피씨 자체의 정보만으로 키를 생성하는 경우에는 이 클라이언트 피씨를 사용하는 사용자는 누구나 정당한 사용자로 간주되어 보안 유지가 어려운 문제점이 있다.

따라서, 상기와 같은 문제점을 감안하여 창안한 본 발명은 사용자의 정보와 클라이언트 피씨의 정보를 이용하여 특정 사용자에 대해서만 인증이 가능하도록 한 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법을 제공함에 그 목적이 있다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위한 본 발명은 사용자 인증요구가 발생하면 클라이언트 피씨 정보와 사용자 정보를 생성하는 제1 단계와; 상기 클라이언트 피씨 정보와 사용자 정보를 조합하여 그에 따른 사용자 암호키를 생성하여 클라이언트 피씨에 내장하는 제2 단계와; 상기 제2 단계의 사용자 암호키를 사용자가 원하는 서버에 등록하는 제3 단계로 수행함을 특징으로 한다.

상기와 같은 목적을 달성하기 위한 본 발명은 사용자 인증 요구가 발생하면 사용자가 원하는 서버로부터 프로그램의 고유 아이디를 다운받아 클라이언트 피씨에 내장하는 제1 단계와; 클라이언트 피씨 정보와 사용자 정보를 생성하는 제2 단계와; 상기 프로그램 고유 아이디와 피씨 정보 및 사용자 정보를 조합하여 그에 따른 사용자 암호키를 생성하여 클라이언트 피씨에 내장하는 제3 단계와; 상기 제3 단계의 사용자 암호키를 사용자가 원하는 서버에 등록하는 제4 단계로 수행함을 특징으로 한다.

이하, 본 발명에 의한 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법에 대한 작용 및 효과를 첨부한 도면을 참조하여 상세히 설명한다.

도1은 본 발명 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법의 실시예에 대한 동작흐름도로서, 이에 도시한 바와같이 사용자 인증요구가 발생하면 클라이언트 피씨에서 피씨 정보와 사용자 정보를 생성하는 제1 단계와, 상기 클라이언트 피씨 정보와 사용자 정보를 조합하여 그에 따른 사용자 암호키를 생성하여 클라이언트 피씨에 내장하는 제2 단계와, 상기 제2 단계의 사용자 암호키를 사용자가 원하는 서버에 등록하는 제3 단계로 이루어지며, 이와 같은 본 발명의 동작을 설명한다.

먼저, 사용자의 인증요구가 발생하면 클라이언트 피씨에서 사용자의 정보를 입력받아 그 사용자의 정보와 클라이언트 피씨의 고유한 정보를 이용하여 유일한 사용자 암호키를 생성하고, 이로 인해 사용자가 자신의 정보를 고의나 불의로 유출하여도 상기 클라이언트 피씨가 아닌 다른 피씨에서는 동일한 사용자 암호키를 생성할 수 없으므로 보안을 해체할 수 없다.

여기서, 도2는 본 발명 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법에 대한 개략도이다.

이때, 상기 사용자 정보로는 사용자의 아이디및 패스워드로 이루어지고, 피씨의 고유한 정보로는 하드 디스크 시리얼 넘버나 씨피유 시리얼 넘버로 이루어진다.

만약, 사용자가 원하는 서버로부터 데이터를 합법적으로 전송받을 때 그 데이터의 불법유출을 방지하기 위하여 클라이언트 피씨에서 생성된 사용자 암호키를 서버에 등록한다.

여기서,보다 상세하게 도3을 참조하여 클라이언트 피씨와 서버 사이에서 사용자키를 사용하여 데이터를 암호화하여 전송하고 복원하는 동작을 설명하면, 우선 클라이언트 피씨는 사용자의 정보를 입력받아 그 사용자의 정보와 클라이언트 피씨의 고유한 정보를 이용하여 유일한 사용자 암호키를 생성한후 그 사용자키를 서버로 전송하여 등록한다.

그러면, 서버는 데이터 암호화키로 전송할 데이터를 암호화하여 헤더영역과 데이터 영역에 저장한후, 상기 등록된 사용자키를 이용하여 상기 데이터 암호화키를 다시 암호화하여 이를 상기 데이터 영역의 뒷부분에 붙여 파일을 형성한다.

여기서, 상기 데이터 암호화키는 일반적으로 데이터를 전송할 때 그 데이터를 암호화하는 키이다.

이후, 상기 서버는 상기 암호화된 파일을 클라이언트 피씨로 전송하게 되고, 이에 따라 상기 클라이언트 피씨는 처음에 생성한 사용자키로 서버에서 사용자키에 의해 암호화된 데이터 암호화키를 복원한후, 그 데이터 암호화키로 헤더영역 및 데이터 영역에 저장된 데이터를 복원한다.

그리고,도4는 본 발명 피씨의 디지탈 콘텐츠 보호용 사용자 암호키 생성방법에 대한 다른 실시예에 대한 개략도로서, 이에 도시한 바와같이 사용자 인증 요구가 발생하면 사용자가 원하는 서버로부터 프로그램의 고유 아이디를 다운받아 클라이언트 피씨에 내장하는 제1 단계와, 클라이언트 피씨 정보와 사용자 정보를 생성하는 제2 단계와, 상기 프로그램 고유 아이디와 피씨 정보 및 사용자 정보를 조합하여 그에 따른 사용자 암호키를 생성하여 클라이언트 피씨에 내장하는

제3 단계와, 상기 제3 단계의 사용자 암호키를 사용자가 원하는 서버에 등록하는 제4 단계로 이루어지며, 이와같은 본 발명의 동작을 설명한다.

먼저, 사용자의 인증요구가 발생하면, 도5의 개략도에서 보는 바와같이 클라이언트 피씨에서 원하는 서버로부터 다운로드 프로그램의 고유아이디와 사용자의 정보를 입력받아 이를 클라이언트 피씨의 고유한 정보와 조합하여 유일한 사용자 암호키를 생성한다.

그러면, 상기의 경우와 마찬가지로 사용자가 자신의 정보를 고의나 불의로 유출하여도 상기 클라이언트 피씨가 아닌 다른 피씨에서는 동일한 사용자 암호키를 생성할 수 없으므로 보안을 해체할 수 없다.

만약, 사용자가 원하는 서버로부터 데이터를 합법적으로 전송받을 때 그 데이터의 불법 유출을 방지하기 위하여 클라이언트 피씨에서 생성된 사용자 암호키를 서버에 등록한다.

여기서, 상기 도1의 경우와 마찬가지로, 사용자 정보로는 사용자의 아이디 및 패스워드로 이루어지고, 피씨의 고유한 정보로는 하드 디스크 시리얼 넘버나 씨피유 시리얼 넘버로 이루어진다.

여기서, 보다 상세하게 도6를 참조하여 클라이언트 피씨와 서버 사이에서 사용자키를 생성한후 데이터를 암호화하여 전송하고 복원하는 동작을 설명하면, 우선 클라이언트 피씨는 서버로부터 프로그램을 다운로그 받아 그 프로그램의 아이디를 이용하여 사용자키를 생성한후 그 사용자키를 서버로 전송하여 등록한다.

그러면, 서버는 데이터 암호화키로 전송할 데이터를 암호화하여 헤더영역과 데이터 영역에 저장한후, 상기 등록된 사용자키를 이용하여 상기 데이터 암호화키를 다시 암호화하여 이를 상기 데이터 영역의 뒷부분에 붙여 파일을 형성한다.

이후, 상기 서버는 상기 파일을 클라이언트 피씨로 전송하게 되고, 이에 따라 상기 클라이언트 피씨는 처음에 생성한 사용자키로 서버에서 사용자키에 의해 암호화된 데이터 암호화키를 복원한후, 그 데이터 암호화키로 헤더영역 및 데이터 영역에 저장된 데이터를 복원한다.

여기서, 도4를 이용한 일반적인 동작은 상기 도1과 거의 동일하다. 다만 서버로부터 프로그램 아이디를 다운받아 이를 사용자키 생성에 이용하므로 특정 프로그램에 대한 데이터 보안에 있어서 탁월한 성능을 가진다.

다시 말하면, 본 발명은 피씨의 고유정보, 다운로드 프로그램의 아이디, 사용자 개인정보를 조합하여 사용자 암호키를 생성함으로써 사용자이외의 사람이 피씨에 접속하여 내장된 정보를 유출할 없도록 하고, 또한 서버로부터 다운받은 콘텐츠를 유출하더라도 동일한 피씨나 동일한 프로그램이 아닌 경우에는 그 콘텐츠를 재생할 수 없도록 하여 불법 복제를 방지한다.

발명의 효과

이상에서 상세히 설명한 바와같이 본 발명은 특정 컴퓨터의 사용자에 의해 생성된 키가 다른 컴퓨터에 복사하더라도 피씨 정보가 틀리므로 처음 키를 생성한 컴퓨터 이외에서는 사용할 수 없고 또한 사용자의 정보가 유출되더라도 최초키를 생성한 컴퓨터가 아니면 동일한 키를 생성할 수 없으므로 확실하게 보안을 유지할수 있고, 그리고 특정 사용자 암호키로 암호화에서 데이터를 전송하면 이 특정 사용자외에는 어느 누구도 데이터를 해독할 수 없으므로 무단 배포를 방지할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

사용자 인증요구가 발생하면 클라이언트 피씨 정보와 사용자 정보를 생성하는 제1 단계와; 상기 클라이언트 피씨 정보와 사용자 정보를 조합하여 그에 따른 사용자 암호키를 생성하여 클라이언트 피씨에 내장하는 제2 단계와; 상기 제2 단계의 사용자 암호키를 사용자가 원하는 서버에 등록하는 제3 단계로 수행함을 특징으로 하는 디지탈 콘텐츠 보호용 사용자 암호키 생성방법.

청구항 2.

사용자 인증 요구가 발생하면 사용자가 원하는 서버로부터 프로그램의 고유 아이디를 다운받아 클라이언트 피씨에 내장하는 제1 단계와; 클라이언트 피씨 정보와 사용자 정보를 생성하는 제2 단계와; 상기 프로그램 고유 아이디와 피씨 정보 및 사용자 정보를 조합하여 그에 따른 사용자 암호키를 생성하여 클라이언트 피씨에 내장하는 제3 단계와; 상기 제3 단계의 사용자 암호키를 사용자가 원하는 서버에 등록하는 제4 단계로 수행함을 특징으로 하는 디지털 콘텐츠 보호용 사용자 암호키 생성방법.

청구항 3.

제1 항 또는 제2 항에 있어서, 피씨정보는 하드 디스크 시리얼 넘버인 것을 특징으로 하는 디지탈 콘텐츠 보호용 사용자 암호키 생성방법.

청구항 4.

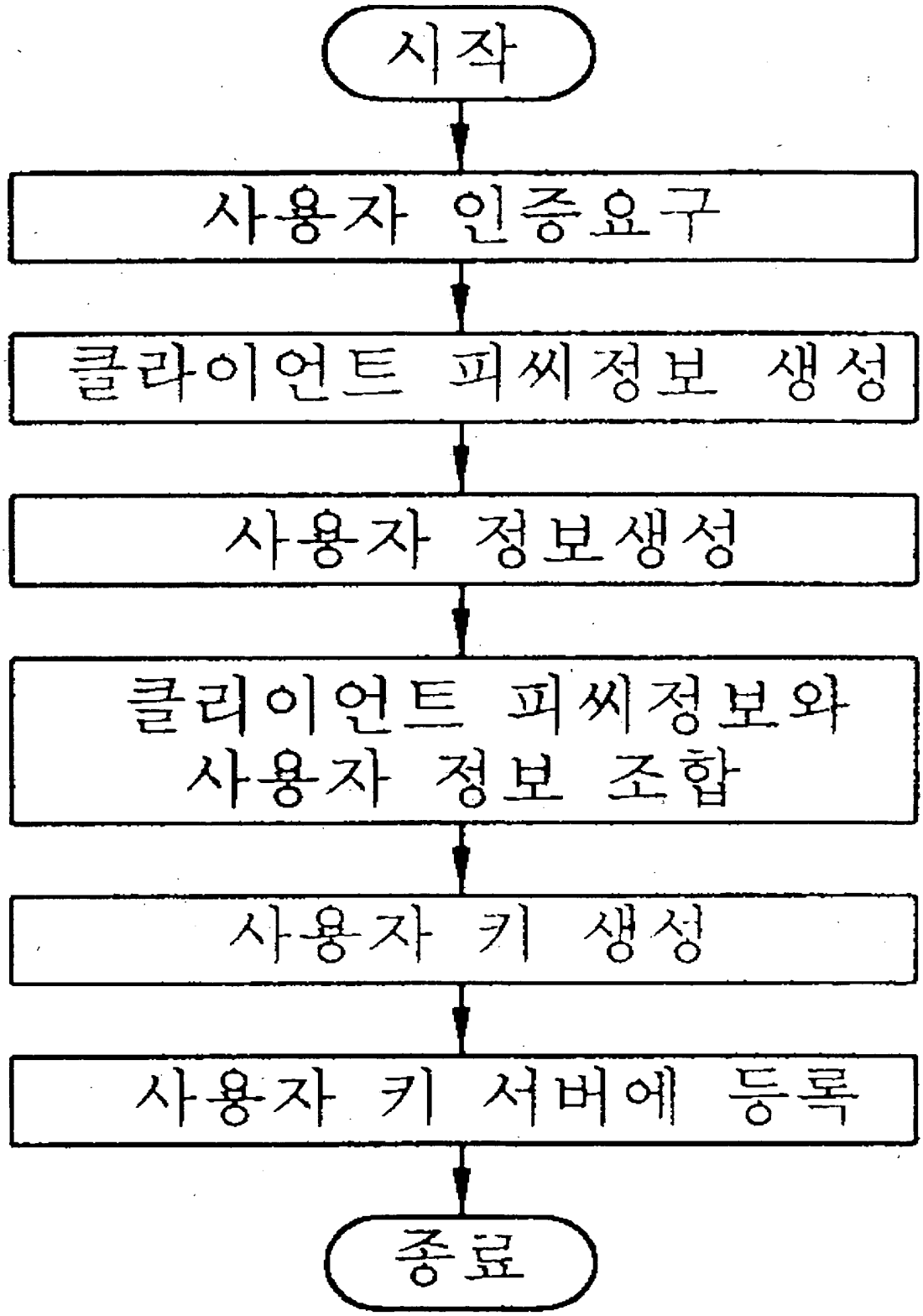
제1 항 또는 제2 항에 있어서, 피씨정보는 씨피유 시리얼 넘버인 것을 특징으로 하는 디지탈 콘텐츠 보호용 사용자 암호키 생성방법.

청구항 5.

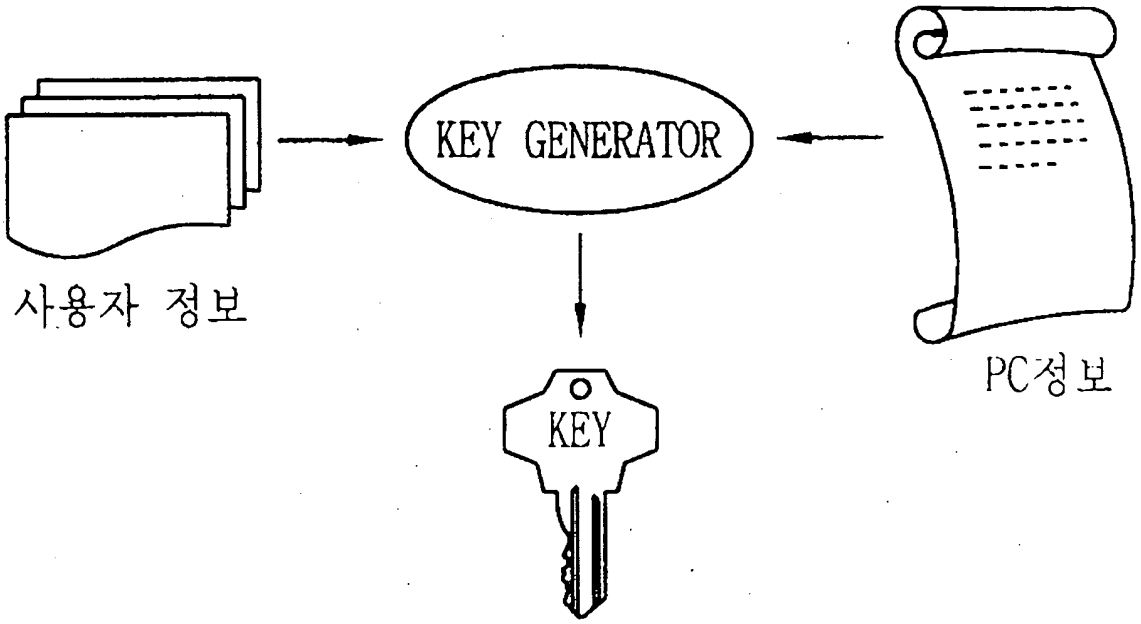
제1 항 또는 제2 항에 있어서, 사용자 정보는 사용자 아이디와 사용자 패스워드로 이루어진 것을 특징으로 하는 디지탈 콘텐츠 보호용 사용자 암호키 생성방법.

도면

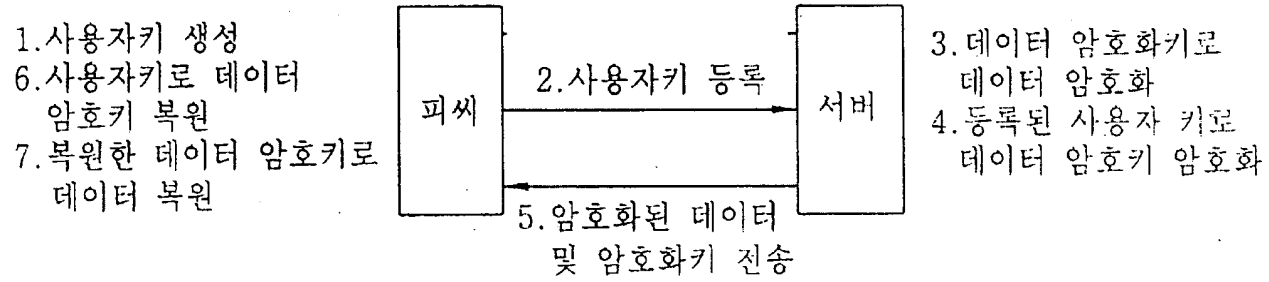
도면 1


시작
사용자 인증요구
클라이언트 피씨정보 생성
사용자 정보생성
클리이언트 피씨정보와
사용자 정보 조합
사용자 키 생성
사용자 키 서버에 등록
종료

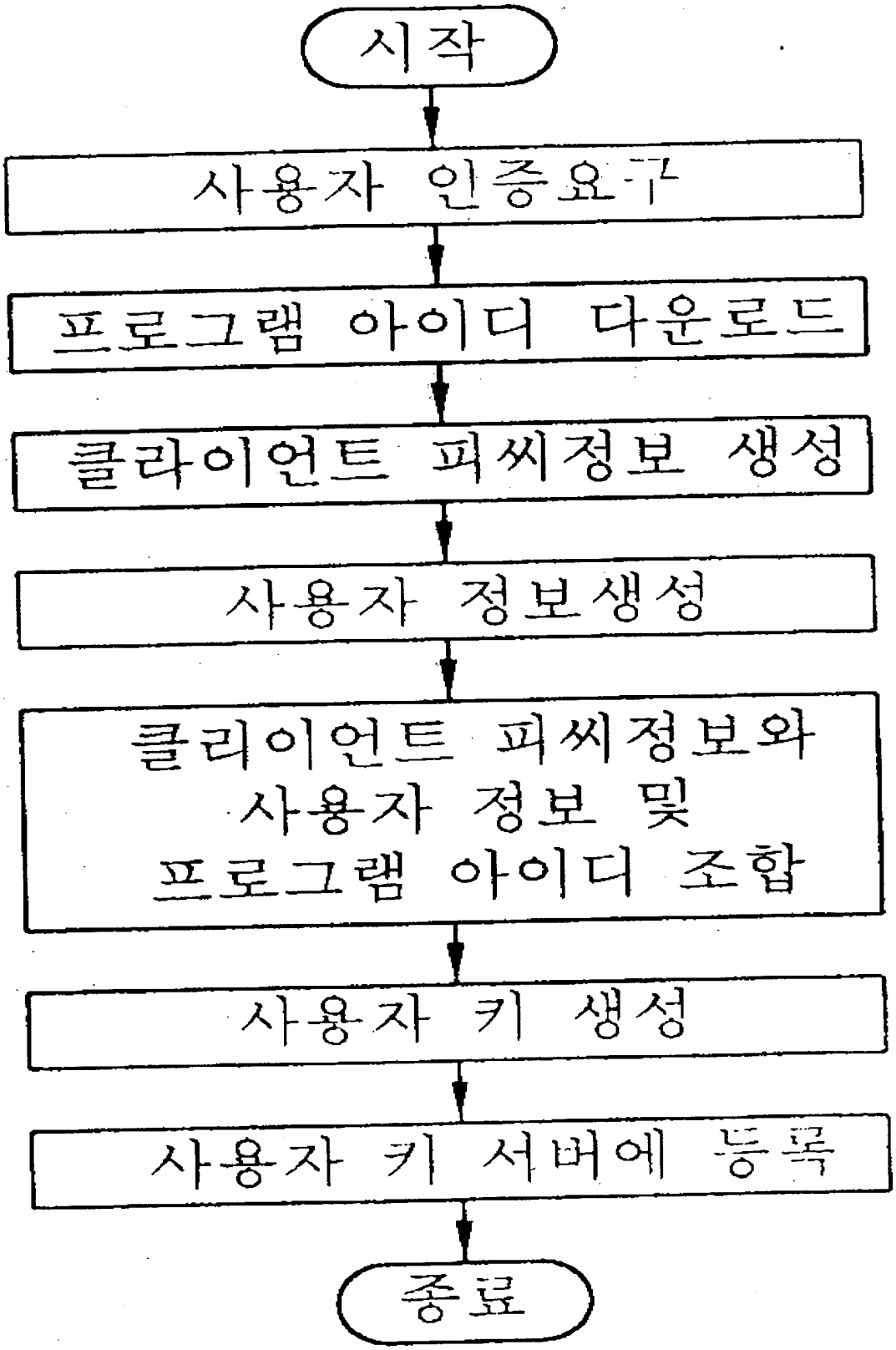
도면 2


KEY GENERATOR
사용자 정보
PC정보
KEY

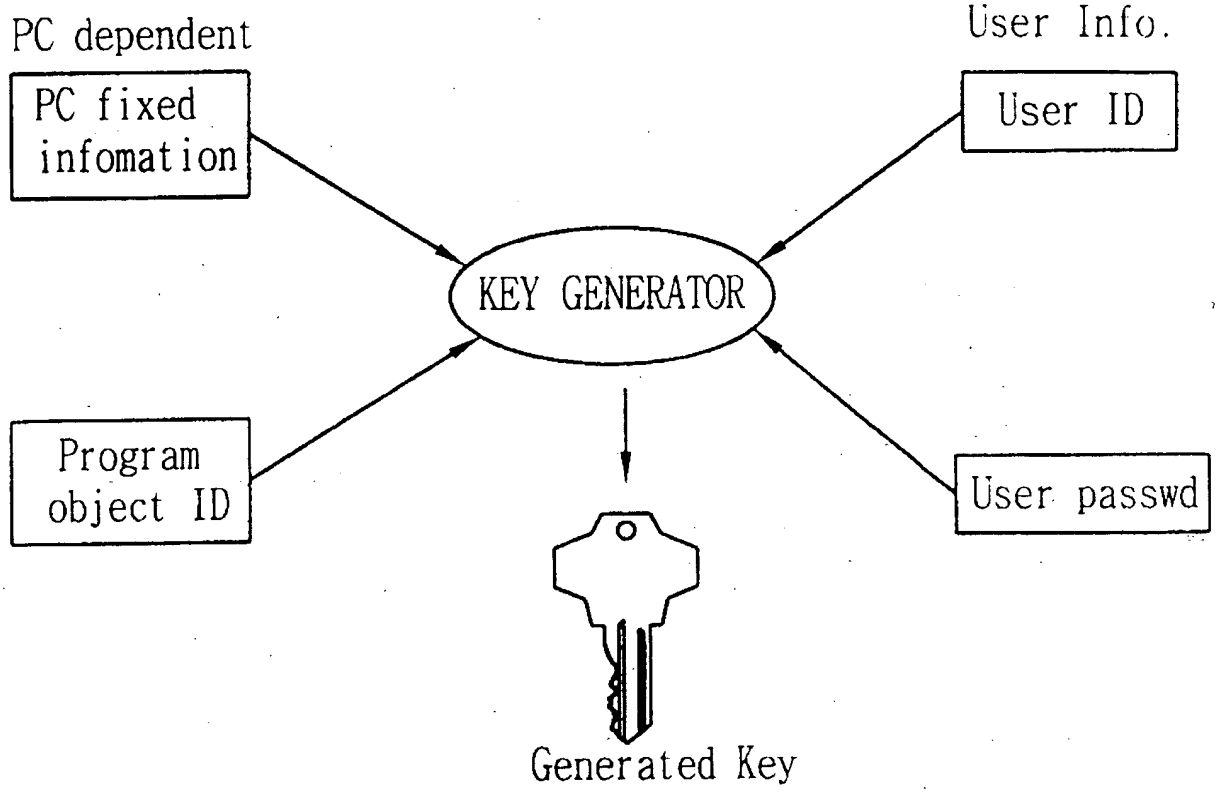
도면 3


1.사용자키 생성
6.사용자키로 데이터
암호키 복원
7.복원한 데이터 암호키로
데이터 복원
피씨
2.사용자키 등록
서버
3.데이터 암호화키로
데이터 암호화
4.등록된 사용자 키로
데이터 암호키 암호화
5.암호화된 데이터
및 암호화키 전송

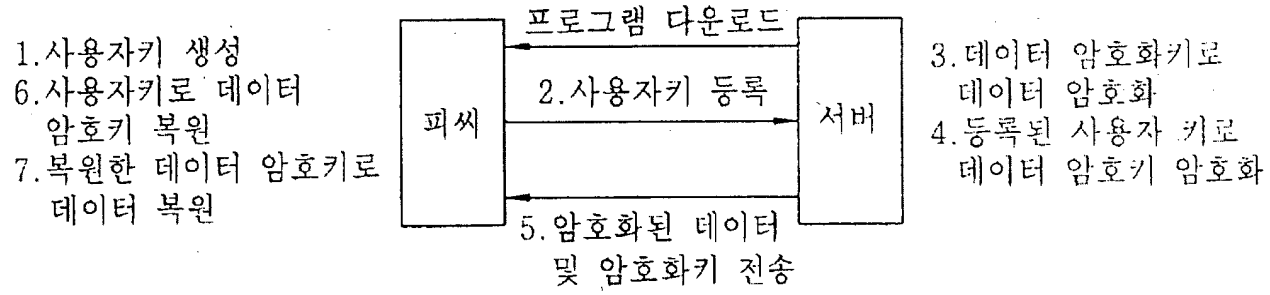
도면 4


시작
사용자 인증요구
프로그램 아이디 다운로드
클라이언트 피씨정보 생성
사용자 정보생성
클리이언트 피씨정보와
사용자 정보 및
프로그램 아이디 조합
사용자 키 생성
사용자 키 서버에 등록
종료

도면 5


PC dependent
PC fixed infomation
User Info.
User ID
KEY GENERATOR
Program object ID
User passwd
Generated Key

도면 6


1.사용자키 생성
6.사용자키로 데이터 암호키 복원
7.복원한 데이터 암호키로 데이터 복원
프로그램 다운로드
2.사용자키 등록
피씨
서버
3.데이터 암호화키로 데이터 암호화
4.등록된 사용자 키로 데이터 암호키 암호화
5.암호화된 데이터 및 암호화키 전송